народной научно-практической конференции «Фундаментальные и прикладные науки сегодня», North Charleston, USA, 2016 г. 199-203 с

2. Смотриков Е.С. Проблемы внедрения автоматизированных информационных систем на современных предприятиях. Труды международной научно-практической конференции «Цифровой Регион: опыт, компетенции, проекты». «Брянский Государственный Инженерно-Технологический Университет» Инженерно-Экономический Институт.2018г

3. Eational Enterprise Management - нформационно-аналитический журнал для руководителей и IT-специалистов промышленных предприятий, научных и проектных организаций.

УДК 004.622

А.С. Шульгина-Таращук, ст. преп.; К.М. Турдыбекова, ст.преп.;
Турдыбекова К.К., студ. (КарГУ им. Е.А. Букетова, г. Караганда)

МЕТОДЫ ШИФРОВАНИЯ ИНФОРМАЦИИ

Шифрование может защитить информацию, электронную почту и другие конфиденциальные данные, а также безопасные сетевые подключения. Сегодня существует множество вариантов на выбор, и обязательно нужно найти безопасный и соответствующий вашим потребностям. Вот четыре метода шифрования и что вы должны знать о каждом из них [1].

The Advanced Encryption Standard, AES - расширенный стандарт шифрования, являющийся симметричным алгоритмом шифрования и одним из самых безопасных. Этот метод использует блочный шифр, который шифрует данные по одному блоку фиксированного размера за раз, в отличие от других типов шифрования, таких как потоковые шифры, которые шифруют данные по битам. AES состоит из AES-128, AES-192 и AES-256. Выбранный вами ключевой бит шифрует и дешифрует блоки 128 битами, 192 битами и так далее. Есть разные раунды для каждого ключа бита. Раунд - это процесс превращения открытого текста в зашифрованный текст. Для 128-битного есть 10 раундов; 192-битный имеет 12 раундов; и 256-битный имеет 14 раундов. Поскольку AES - это шифрование с симметричным ключом, вы должны предоставить этот ключ другим лицам, чтобы они могли получить доступ к зашифрованным данным. Кроме того, если у вас нет безопасного способа поделиться этим ключом, и посторонние лица получают к нему доступ, они могут расшифровать все, что зашифровано с помощью этого конкретного ключа.

Triple Data Encryption Standard, 3DES - тройной стандарт шифрования данных, являющийся текущим стандартом и является блочным шифром. Это похоже на более старый метод шифрования, Data Encryption Standard, который использует 56-битные ключи. Однако 3DES - это шифрование с симметричным ключом, в котором используются три отдельных 56-битных ключа. Он шифрует данные три раза, что означает, что ваш 56-битный ключ становится 168-битным ключом. К сожалению, поскольку он шифрует данные три раза, этот метод намного медленнее других. Кроме того, поскольку 3DES использует меньшую длину блоков, легче расшифровывать и пропускать данные. Однако многие финансовые учреждения и предприятия во многих других отраслях используют этот метод шифрования для обеспечения безопасности информации. По мере появления более надежных методов шифрования этот метод постепенно удаляется.

Twofish - это симметричный блочный шифр, основанный на более раннем блочном шифре - Blowfish. Twofish имеет размер блока от 128 до 256 бит и хорошо работает на небольших процессорах и оборудовании. Подобно AES, он реализует циклы шифрования для превращения открытого текста в зашифрованный текст. Тем не менее, количество раундов не меняется, как с AES; независимо от размера ключа всегда есть 16 раундов. Кроме того, этот метод обеспечивает большую гибкость. Вы можете выбрать медленную настройку ключа, но процесс шифрования будет быстрым или наоборот. Кроме того, эта форма шифрования не имеет патентов и лицензий, поэтому вы можете использовать ее без ограничений.

RSA - этот асимметричный алгоритм назван в честь Рона Ривеста, Ади Шамира и Лена Адельмана. Он использует криптографию с открытым ключом для обмена данными по небезопасной сети. Есть два ключа: один публичный и один закрытый. Открытый ключ, как следует из названия: открытый. Любой может получить к нему доступ. Однако закрытый ключ должен быть конфиденциальным. При использовании криптографии RSA вам необходимо использовать оба ключа для шифрования и дешифрования сообщения. Вы используете один ключ для шифрования ваших данных, а другой - для его расшифровки. Согласно Search Security, RSA является безопасным, потому что он учитывает большие целые числа, которые являются продуктом двух больших простых чисел. Кроме того, размер ключа большой, что повышает безопасность. Большинство ключей RSA имеют длину 1024 и 2048 бит. Однако более длинный размер ключа означает, что он медленнее, чем другие методы шифрования.

В то время как существует множество дополнительных методов шифрования, знание и использование самых безопасных из них гарантирует, что ваши конфиденциальные данные остаются в безопасности и вдали от нежелательных глаз.

ЛИТЕРАТУРА

Никифоров, С. Н. Методы защиты информации. Пароли, скрытие, шифрование/ С. Н. Никифоров. – Санкт – Петербург: Лань, 2018. – 124 с.

УДК 004.738

Р.И. Допира, ст. преп.; Н.В. Попова, ст. преп.
(Карагандинский государственный университет
имени академика Е.А. Букетова, Караганда, Казахстан)

ФОРМИРОВАНИЕ КОМПЕТЕНЦИЙ IT-СПЕЦИАЛИСТА ПРИМЕНЯЯ МЕТОД ПРОЕКТОВ НА ЗАНЯТИЯХ СРСП ДИСЦИПЛИНЫ «ПРОГРАММИРОВАНИЕ НАС++»

Реформирование образовательного пространства предполагает оптимизацию содержания и форм педагогической деятельности, внедрение инновационных технологий в образовательный процесс. Одна из форм педагогической деятельности обеспечивающих профильное обучение – это метод проектов. Метод проектной деятельности активизирует самостоятельную работу обучающихся, направленную на поиск информации и получение практического результата, развивает творческие способности.

Работа над проектами со студентами проводилась на занятиях по дисциплине «Программирование наС++» во время самостоятельной работы студентов под руководством преподавателя. Учащимся было предложено разработать проект, взяв за основу имеющиеся у них знания, полученные за пройденный курс «Технология программирования». Совместно со студентами был разработан план создания проектов, который содержал в себе: формирование состава проектных групп и первичное распределение обязанностей среди группы; формулировка темы проекта, постановка задач, определение конечного вида создаваемого программного продукта, его назначение; выбор программного обеспечения; выделение подзадач для определенных групп учащихся, подбор необходимого материала; непосредственно работа над проектом; подведение итогов.

На первом этапе студенты разбивались на группы, каждая из которых должна разработать собственный проект. Они самостоятельно выстраивали план работы над проектом. На каждом этапе работы обу-